



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/528,312	03/17/2005	Markus Franke	2002P15289WOUS	2692
7590 Siemens Corporation Intellectual Property Department 170 Wood Avenue South Iselin, NJ 08830				
EXAMINER				
HAILU, TESHOME				
ART UNIT		PAPER NUMBER		
2439				
MAIL DATE		DELIVERY MODE		
04/10/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/528,312

Applicant(s)

FRANKE ET AL.

Examiner

TESHOME HAILU

Art Unit

2439

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 December 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 6, 8, 10, 12, 14, 16, 18, 20, 22 and 23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 6, 8, 10, 12, 14, 16, 18, 20 and 22-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This office action is in reply to an amendment filed on December 18, 2008. Claims 6, 8, 10, 12, 14, 16, 18, 20, 22 and 23 have been amended.
2. Claims 6, 8, 10, 12, 14, 16, 18, 20, 22 and 23 are pending.
3. Claims 1-5, 7, 9, 11, 13, 15, 17, 19 and 21 have been cancelled.

Response to Amendment

4. Applicant's arguments with respect to claims 6 and 18 have been fully considered but they are not persuasive.
5. Applicant argues that Oka (US Pub. No. 2002/0108042) fails to teach the claim limitation, "performing a certification of the public validation key wherein, when validating, only those signatures generated at a time prior to the certification of the public validation key are recognized as valid signature". Examiner respectfully disagrees.
6. Examiner would point out that, Oka teach this limitation as (page 12, paragraph 193, fig. 22 shows an example in which the end entity (EE) 300 outputs a public key certificate issuance request to the registration authority (RA1) 311. Numerals (1) through (10) in FIG. 22 represent steps to be taken by the parties involved. These steps are described below in ascending order). According to Oka, the end entity (EE) sends the public key certification issuance request to certificate authority server through registration authority. Then the certificate authority execute signature using hardware security module (HSM). The CA check whether the signature is valid or not and then if it is judged valid, the CA sends the public key certificate to end entity (EE) through registration authority. Here validating the signature by CA takes place before certifying the public key. Once the signature is valid, the CA sends the public key

certificate to end entity (meaning first validating the signature and then certifying the public key). Also see paragraph 193-203 and fig. 22. According to the steps on fig. 22, the signature verified (step 8) before the certificate is issued (step 9). Examiner asserts that the art on record teaches the claim limitations as discussed in the previous office action and therefore the rejection is respectfully maintained.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 6, 8, 10, 12, 14, 16, 18, 20, 22 and 23 are rejected under 35 U.S.C. 102(b) as being anticipated by Oka (Oka) (US Pub. No. 2002/0108042).

As per claim 6 Oka discloses:

A method for generating and/or validating electronic signatures, the method comprising: (page 3, paragraph 31, certificate authority may have a verification key database which stores keys for signature verification in association with each of the plurality of signature modules; and the certificate authority may verify signatures by each of the plurality of signature modules).

Generating an asymmetrical key pair which includes a private signature key and a public validation key; (page 2, paragraph 13, the certificate authority also generates public and private keys as needed).

Calculating an electronic signature for an electronic document by means of the private signature key and by applying a predeterminable signature function; (page 1, paragraph 9, the user A also attaches signatures to the documents using the private key. The indefinite number of users goes through the

predetermined procedure to obtain the public key from the public key certificate and have the attached signatures verified).

Performing a certification of the public validation key wherein, when validating, only those signatures generated at a time prior to the certification of the public validation key are recognized as valid signature. (page 12, paragraph 193, fig. 22 shows an example in which the end entity (EE) 300 outputs a public key certificate issuance request to the registration authority (RA1) 311. Numerals (1) through (10) in FIG. 22 represent steps to be taken by the parties involved. These steps are described below in ascending order). Also see paragraph 193-203 and fig. 22. According to the steps on fig. 22, the signature verified (step 8) before the certificate is issued (step 9).

Claim 18 is rejected under the same reason set forth in rejection of claim 6:

As per claim 8 Oka discloses:

The method according to Claim 6, wherein, when certifying the public validation key, a reference to the electronic document is included in addition to a user identifier and the public validation key. (page 1, paragraph 11, A typical public key certificate shown in FIG. 1 includes: a certificate version number; a serial number allocated to a certificate user by a certificate authority (CA); algorithm and parameters used for signature by the RSA, ECDSA, etc.; a certificate authority name; the period of certificate validity; the certificate user's name (user ID); the user's public key; and a digital signature).

Claim 20 is rejected under the same reason set forth in rejection of claim 8:

As per claim 10 Oka discloses:

The method according to Claim 8, wherein an implementation of the reference is performed by a calculation of a hash value for the electronic document. (Page 1, paragraph 12, a hash value is generated using hash function, and the certificate authority's private key is applied to the hash value to generate the signature). Also see fig. 1.

Claim 22 is rejected under the same reason set forth in rejection of claim 10:

As per claim 12 Oka discloses:

The method according to Claim 6, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document. (Page 13, paragraphs 201-203, the CA server 321 retrieves a verification key from the verification key database to check whether the signature on the received public key certificate is valid. If the signature is judged valid, the CA server 321 sends the signed public key certificate to the requesting registration authority (RA1) 311. In turn, the registration authority (RA1) 311 forwards the signed public key certificate received to the requesting end entity (EE) 300).

Claims 14, 16, and 23 are rejected under the same reason set forth in rejection of claim 12:

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TESHOME HAILU whose telephone number is (571)270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2439

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Teshome Hailu/

Examiner, Art Unit 2439

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434